Executive Summary for Migrating to a Total Private IP Network within Kentucky Schools

A KETS Implementation Document

Scope of Document:

The scope of this document is to provide guidance for Kentucky School Districts as they change from a mixed IP environment to a total Private IP environment. This summary is not meant to be a step by step implementation guide, but rather to provide a road map for districts as they prepare and proceed with the conversion to Private Networks.

Note:

This document is written and designed for districts that have a point to point T1 connection to Frankfort.

Scope of Issue:

The restructuring of the new IP addresses and scheme has been adopted to accommodate the growing needs for unique IP addresses statewide. The use of private IP offers several advantages to include security, an increased number of devices available on the network, and network stability.

Typically, when a district implements private IP ranges at a school, they assign a public range and a private range to each school. Although there is one physical network in the school, there are now two logical networks (the public range and the private range). This is a common practice and is referred to as multinetting.

When multinetting in the KETS environment, both the public and private ranges will behave the same, and will be able to directly reach any valid IP address on the Internet. Any public number will also be able to reach any private number within the district, even between schools. The private numbers will be able to communicate directly with any public or private number within that school district, *and* between schools. However this

multinetting practice does not behave well with certain applications and network services. Also, this design provides a more complex network structure.

KDE has enabled routing of private IP addresses statewide. Also, KDE has implemented a static and dynamic Network Address Translation (NAT) at the State Level so that all computers can initiate connections out to the Internet and can be seen from the Internet. Lastly, KDE has deployed internal DNS (Domain Name Service) servers that will allow Private DNS translations internally to the state.

Because of these implementations, districts may now move forward with converting their networks to a single IP network and have a totally private network without losing any functionality of their existing networks.

Explanation of IP Division and Guidelines:

Rules of IP Divisions

1. Each district is given at least one Class B address range.
2. The Class B address range is divided into 16 Class C address ranges for each school in every district – giving each school 4080 private addresses.
3. The first and last set of 16 Class C address ranges are not assigned in every Class B and can be used for future growth of the district at a later date.
4. The district Board Office is allocated the second set of 16 Class C address ranges in every district.
5. Under this division every computer can use the same subnet mask of 255.255.240.0
6. The first Class C range is reserved for servers and network devices.
7. The second Class C range is reserved for workstations and perhiphial devices that need a staticly assigned IP address.
8. The 3rd through the last Class C range is reserved for DHCP
9. Ranges for the other networks such as Nortel Net Knowledge – Cisco Academy – STLP Labs – etc… were defined as follows

    * Cisco Academy – Must use 172.16.x.x IP Addressing because of the use of Active Directory in the Cisco Academy Classes, along with the hardware not being a KETS standard hardware.
    * STLP Labs, etc… - Must also use this range for the same reasons. However STLP Labs that do not intend to participate in any Directory Services outside the realm of their districts Directory Services may use the school's Private IP addressing scheme.
    * Nortel Net Knowledge – May use the School's Standard Private IP addressing scheme if the district intends to use the lab for other purposes than that of the Nortel Class. However, if the lab is intended for just the use of the Nortel class then the class can use either the 172 range or the

standard Private ranges assigned to the school. ** Note – the Nortel Curriculum must be changed to address the new ranges.

The following list represents the assigned addresses as identified in the KETS IP Assignment Standards document for the 1st Class C in every range.

```
10.x.x.1 ---------------------- Default Gateway Device
10.x.x.2 ---------------------- Backbone CSU/DSU
10.x.x.3 ---------------------- Secondary Gateway Device
10.x.x.4-9 -------------------- RESERVED
10.x.x.10 --------------------- MUNIS
10.x.x.11 --------------------- Exchange (Mail)
10.x.x.12 --------------------- STI Accumulator (Priority)
10.x.x.13 --------------------- School STI Server
10.x.x.14 --------------------- District Proxy
10.x.x.14[1] ------------------ School Proxy
10.x.x.15[1] ------------------ School Proxy
10.x.x.16-49 ------------------ Active Components[2]
10.x.x.50 --------------------- Global Catalog Server (GC)
10.x.x.50 --------------------- DNS (GC)
10.x.x.50 --------------------- WINS (GC)
10.x.x.50-59 ------------------ .NET Controllers
10.x.x.60-90 ------------------ Web Servers
10.x.x.91-99 ------------------ FTP Servers
10.x.x.100 -------------------- Webmail [dedicated]
10.x.x.101 -------------------- Student Webmail [dedicated]
10.x.x.111 -------------------- Student Exchange (Stu Mail)
10.x.x.112-224 ---------------- Unassigned
10.x.x.225-244 ---------------- Downstream CSU/DSUs

10.254.x[3].0 ------------------ Router WAN Ports
```

[1] School proxy will be .14 unless it is on the same subnet as the district proxy in which case school proxy will be assigned .15

[2] Switches, Hubs, Active/managed Network Components, WAP, etc.

[3] Assigned District Office Class B

Example:

No.	District Name	No.	School Name	Public IP Range	Private IP Range	Gateway	Mask
1	ADAIR CO.	000	District Office	170.180.183.193-254	10.21.16.1 - 10.21.31.254	10.21.16.1	255.255.240.0
1	ADAIR CO.	010	ADAIR COUNTY HS	170.180.180.1-254	10.21.32.1 - 10.21.47.254	10.21.32.1	255.255.240.0
1	ADAIR CO.	095	CASEY EL	170.180.181.1-254	10.21.48.1 - 10.21.63.254	10.21.48.1	255.255.240.0
1	ADAIR CO.	170	JOHN ADAIR MID	170.180.182.1-254	10.21.64.1 - 10.21.79.254	10.21.64.1	255.255.240.0

1	ADAIR CO.	240	KNIFLEY EL	170.180.183.129-190	10.21.80.1 - 10.21.95.254	10.21.80.1	255.255.240.0
1	ADAIR CO.	435	SHEPHERD EL	170.180.183.65-126	10.21.96.1 - 10.21.111.254	10.21.96.1	255.255.240.0
1	ADAIR CO.	460	SPARKSVILLE EL	170.180.183.1-62	10.21.112.1-10.21.127.254	10.21.112.1	255.255.240.0
5	ALLEN CO.	000	District Office	170.180.175.129-190	10.22.16.1 - 10.22.31.254	10.22.16.1	255.255.240.0
5	ALLEN CO.	010	ALLEN CO PRIMARY	170.180.172.1-254	10.22.32.1 - 10.22.47.254	10.22.32.1	255.255.240.0
5	ALLEN CO.	015	JAMES E BAZZELL MS	170.180.174.1-254	10.22.48.1 - 10.22.63.254	10.22.48.1	255.255.240.0
5	ALLEN CO.	020	ALLEN COUNTY HS	170.180.173.1-254	10.22.64.1 - 10.22.79.254	10.22.64.1	255.255.240.0
5	ALLEN CO.	060	WHITE PLAINS EL	170.180.175.1-126	10.22.80.1 - 10.22.95.254	10.22.80.1	255.255.240.0
5	ALLEN CO.	901	ALLEN CO VOC ED	170.180.175.193-254	10.22.96.1 - 10.22.111.254	10.22.96.1	255.255.240.0
6	ANCHORAGE	000	District Office	170.181.179.1-62	10.23.16.1 - 10.23.31.254	10.23.16.1	255.255.240.0
6	ANCHORAGE	010	ANCHORAGE EL	170.181.178.1-126	10.23.32.1 - 10.23.47.254	10.23.32.1	255.255.240.0
6	ANCHORAGE	020	ANCHORAGE MS	170.181.178.129-190	10.23.48.1 - 10.23.63.254	10.23.48.1	255.255.240.0
6	ANCHORAGE	030	9TH GRADE CTR	170.181.178.193-254	10.23.64.1 - 10.23.79.254	10.23.64.1	255.255.240.0

The Entire Spreadsheet can be acquired from the KETS Help Desk

---

Document Road Map:

First:

A district must define what ranges that they have and verify that all ranges are on its appropriate layer three switches and routers in accordance with the standards that have been established by OET. These ranges can be acquired by the appropriate KRE for each region. If ranges are not on the routing devices, the District should notify the KRE for their region as to what ranges need to be added and to which devices. The KRE will then take the appropriate actions to ensure that the ranges are added, and notify the district of its completion.

Second:

Create a DNS form to supply to the KRE with a one to one correlation of all servers that exist in the district's internal network as defined by the last column of the form. If a service exists that is not named, please include it. If a server doesn't have a private IP address associated with it, please reserve an address for that server and include it in the document to keep everyone from having to go back and put it in later. This form should look similar to the excerpt below…

District XYZ
DNS Table

NetBios Name	***Current Public IP Address***	***Private IP Address***	***Services Running &DNS NAME***
	170.181.10.3	10.132.16.2	CSU
E176030N0	170.181.10.130	10.132.16.14	Proxy proxy.district.k12.ky.us
E176030N1	170.181.10.131	10.132.16.10	RS6000
E176030F2	170.181.11.16	10.132.16.11/ 50	Exchange, DNS, WINS mail.exchange.k12.ky.us
E176040N0	170.181.11.4	10.132.64.14	Proxy proxy.school.district.k12.ky.us
E176040N1	170.181.11.6	10.132.16.60	AWS, Webmail, WWW www.district.k12.ky.us webmail.district.k12.ky.us
E176040N2	170.181.11.5	10.132.16.111	StuMX stu.mail.district.k12.ky.us
E176040F1	170.181.11.197	10.132.32.14	Proxy proxy.school.district.k12.ky.us
E176011N0	170.181.11.17	10.132.16.120	DHCP
E176011N1	170.181.11.7	10.132.16.13	STI Accumulator
E176010N0	170.181.9.252	10.132.48.14	Proxy proxy.school.district.k12.ky.us

This allows for the Networking team to input the private IP address into the External DNS tables for those servers that require a one to one translation and also allows for the Internal DNS tables to be built for district to district DNS translations and for Static NAT rules to be made.

Questions regarding what should be included in the DNS table that are submitted to the Networking Team can be answered with the accompanying file "The Role of a District's DNS Defined".

Third:

Begin the conversion of workstations and printers and periphial devices to the new private ranges. Items that can should be converted should include CDRom Towers/Wireless Access Points/Hardware Devices, such as Shiva's/Caching Devices/RAS devices/VPN Boxes. A district should also convert servers/workstations that do not need access to the world via DNS Entries or host files.

> Note: (Servers/Workstations that need such entries would include but not be limited to Exchange Servers, Web Server, RS6000 accessible workstations and printers, Real Media Servers and Servers that require reverse DNS Authentication) - (Servers that may require reverse DNS Authentication could include but not be limited to, Weather Collection Servers, Content Filtering Servers, Internet Testing Servers, HVAC Servers, etc…)

Example of servers that could be converted could include but not be limited to DHCP Servers, STI Servers, Domain Controllers, etc… This step can be performed without making any prior request or call to the KETS Help Desk or KETS Network Team, as long as both ranges are on all routing devices as stated in step one.

DHCP Servers should be set to distribute the IP addresses from the 3rd Class C on with a DNS and WINS Server of 10.X.X.50.

Fourth:

Multinet All Servers that require DNS and Host File authentication. With the primary IP address being the private IP and the Secondary Number being the public IP address.

> Note: WINS Server's (Exchange Server) primary IP address should be .50 with the secondary IP address being the .11 private and the existing public address.

Microsoft Proxy Servers must have their LAT (Local Address Table) Tables updated to include the new ranges of private IPs. Also, if a district is using IP Restrictions to its proxy server, they must also add the new ranges into the allow rule in order for the workstations to communicate to the proxy server on the new ranges.

For instructions on how to multinet a device please refer to the document Multinetting NIC that accompanies this summary.

Fifth:

Schedule a time with the appropriate KRE to have them onsite for your cutover date. The final steps should be completed with the KRE onsite to assist and oversee the final implementation.

Sixth:

Check the DNS Server. The districts steps involve the following: from the District DNS server check the DNS zone to verify the private ranges are being advertised. Follow the instructions below for checking the DNS server.

- Click Start -> Programs -> Admin Tools ->DNS Admin
- The DNS Admin Tool will Start
- Click on the Current DNS Zone and it will highlight
- Right Click the Zone
- Click Properties
- Verify that Forwarding is enabled and 10.16.1.1 is the listed server
- Finally Verify that the zone lists the private ranges as requested to the Networking Team.
- If any of the verification points fail, contact the Networking Team for immediate resolution.
- Exit DNS Admin

  ** Note – Windows XP and Windows 2000 Clients and Servers may have to do a DNS Flush to remove any cached DNS entries in their local cache. This can be performed by going to a DOS Prompt and typing "ipconfig /flushdns"

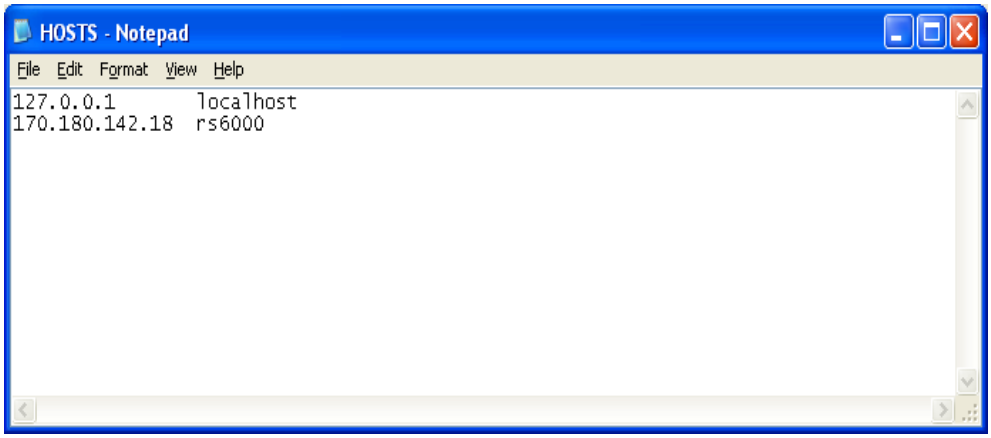
Seventh:

Convert the RS6000 servers and accompanying workstations and printers. This step involves the District, KRE, KETS Help Desk, Networking Team, and MUNIS Team. The instructions are included in the documents that accompany this file.

Also, ensure that any third party vendor software such as PSST is not affected by this change. Many accompanying software require hosts files or third party software, that must be edited in order to allow the computers to interact with the new ranges.

Note* The following instructions to changing a Host file on a Windows workstation are below.

1) Click Start -> Search -> for Files or Folders
2) Type "hosts" and click Search
3) Double click the file when the search finds the file. *Note – do not open the hosts.sam file. Open the hosts file
4) If your computer ask you for a program to open the file with, choose Notepad
5) The file will open and it will look like the below screen possibly with the rs6000 listed as one of the entries in the list.



6) If the entry is in the list, remove the old number and put the new IP address of the RS6000 in the same place with a tab key separating the ipaddress and the name of the server
7) Click File -> Save and exit the Notepad Program.

Eighth:

Convert the Exchange Server. This step involves the District, KRE, Messaging Team and the Networking Team. The districts steps involve the following:

- In Step Four the IP addresses of the Exchange Server were placed in the following order: .50 (Private) .11 (Private) 170.x (Public)
- Remove the Public IP Address from the Exchange Server.
- Contact the Messaging Team to have them point the X400 Connectors to the Private Address.
- After the Messaging Team has changed the X400 Connectors, contact the Networking Team to change the WINS entry for the district.

Ninth:

Take all public IP addresses off of all multinetted devices in the district. The only exceptions are VPN Servers hosted in the District. These devices must reside at the hub site at the current time will be able to continue to have a public IP Address.

Tenth:

Remove all public ranges off of any router and layer three switches with the exception of the District Hub Router and the accompanying CSU/DSU. Once completed, this will result in only a private range existing on any layer three switch or router with the exception of the Hub Site Router, CSU and Sync port of the BCN, which will be handled by the Networking Team and GOT.